>>> "Hal Amens" <hal@lpf.com> 02/15/03 03:57PM >>>
The HIPAA Implementation Newsletter
Issue #51 – Friday, February 14, 2003
| Security | Transactions | Status | Enforcement | Internet | Privacy | Bankruptcy | Certification?
Web format with links at http://lpf.com/hipaa/

Security: Final Standards

"Under the [final] security standards … health insurers, certain health care providers and health care clearinghouses must establish procedures and mechanisms to protect the confidentiality, integrity and availability of electronic protected health information. The rule requires covered entities to implement administrative, physical and technical safeguards to protect electronic protected health information in their care.
"The security standards work in concert with the final privacy standards adopted by HHS last year and scheduled to take effect for most covered entities on April 14. The two sets of standards use many of the same terms and definitions in order to make it easier for covered entities to comply.
"The security standards will be published as a final rule in the Feb. 20 Federal Register with an effective date of April 21, 2003. Most covered entities will have two full years -- until April 21, 2005 -- to comply with the standards …"
+ More at: http://www.hipaadvisory.com/news/2003/0213hhs.htm and The complete text of the Security Final Rule (PDF).

Transactions: Updated Final Rule:

The final transaction modifications rule, which will also be published in the Federal Register on Feb. 20, combines two proposed rules published May 31, 2002. Major provisions of the final rule include:

- Repealing the National Drug Code (NDC) as the standard medical data code set for reporting drugs and biologics in all non-retail pharmacy transactions.

- Continuing the use of the NDC code set for the reporting of drugs and biologics for retail pharmacy transactions.

- Adopting the National Council for Prescription Drug Programs (NCPDP) Batch Version 1.1 to support the Telecommunications Version 5.1.

+ More at: http://www.hipaadvisory.com/news/2003/0213hhs.htm and the complete text of the Transaction Modification Final Rule Acrobat (PDF) or Web page (HTML).

Transactions: CAQH and WEDI Web Site

"Created by the Council for Affordable Quality Healthcare (CAQH) and the Workgroup for Electronic Data Interchange (WEDI), a new web site intends to ease potential provider confusion related to 2003 HIPAA- and NCPDP-mandated changes in health plan-provider electronic interactions. Designed as one common resource for providers and plans alike, the site gives providers information on health plan transaction changes and equips health plans with tools to communicate these changes to providers. Participation and use of the site is free."
+ More at: http://www.wedi.org/snip/caqhimptools/

Status: Winter HIPAA Survey

"Only nine percent of healthcare providers and five percent of payers have met the looming April 14 deadline to comply with the HIPAA Privacy remediation and the Transactions and Code Sets (TCS) testing deadline. These results were presented in the Winter 2003 U.S. Healthcare Industry Quarterly HIPAA Compliance Survey conducted by the Healthcare Information and Management Systems Society (HIMSS) and Phoenix Health Systems, Inc. Additional findings include:

- Compliance Figures: The winter survey results show little change from the fall survey results with only nine percent of healthcare providers and five percent of payers meeting the [privacy] compliance deadline. … an additional 75% of the providers (total of 84%) reported that they will be ready in time
- Deadline Extension: Ninety percent of respondents reported they have applied for the Transactions deadline extension of October 2003.
- Testing: Only six percent of providers and 11 percent of payers have actually completed TCS remediation efforts. Only 37 percent expect to be ready for testing in April 2003. Forty two percent of providers have not decided on their Transactions testing strategies.
- Half of the survey participants have begun security assessment.

"'With the deadline less than three months away, it's apparent that many healthcare organizations report that compliance is moving ahead, but progress is slow,' said D'Arcy Guerin Gue, executive vice president, Phoenix Health Systems. 'But the challenge remains in changing the overall culture of the organizations to gain acceptance.'"
+ More at:
http://www.himss.org/ASP/ContentRedirector.asp?ContentId=27584 and
http://www.modernphysician.com/news.cms?newsId=498

Enforcement: FY 2004 Budget

"The Centers for Medicare and Medicaid Services (CMS) and the Office for Civil Rights (OCR) would receive funds in fiscal year 2004 specifically

earmarked for enforcing HIPAA, according to President George W. Bush's proposed budget for the Department of Health and Human Services. The budget would provide CMS with $10 million to enforce the transactions and code sets, security and identifier provisions and would provide OCR with $34 million to enforce the privacy rule.

OCR is slated to use its funds to 'support the investigative, legal and related administrative expenses associated with implementing compliance with and enforcement of the HIPAA privacy rule,' according to the document."
+ More at: http://thompson.com/libraries/healthcare/safe/index.html

Internet: Kaiser Patient Records Online

"Kaiser Permanente, the nation's largest non-profit health maintenance organization, Tuesday said it is embarking on a three-year plan to put 8.5 million of its members' patient records online. The Oakland, Calif.-based HMO said it will spend upwards of $1.8 billion on its revised Automated Medical Records (AMR) platform to make what it claims is the 'largest ever transition to a paperless medical record system.'
"When finished, patients, physicians and other authorized health care staff will have access to up-to-the-minute medical records, including test results. Kaiser said patients would also be able to schedule appointments, request medication refills, and ask for referrals with a few short clicks of the mouse.
…
"As for hacker attacks, Kaiser said the AMR uses tools to protect against unauthorized remote access, with security checks and audits within multiple layers of the system. 'We are committed to protecting our patients' privacy and fully complying with government privacy provisions. That is why we selected a system with state-of-the-art security, with many levels of password protection,' said Permanente Federation executive director Francis J. Crosson, M.D."
+ More at: http://www.internetnews.com/ent-news/article.php/1579261

Privacy: Chief Privacy Officers

"The chief security officer (CSO) position has matured to the point where the title isn't particularly jarring when you see it on a business card. However, the same probably cannot be said for the chief privacy officer (CPO) job. "… as companies face increasing pressure from the public to keep data protected, they are creating CPO positions. The move has both organizational and public relations value. For example, IBM Corp. got a lot of coverage in 2000 when it named Harriet Pearson CPO in order to, in the company's words, 'lead initiatives across IBM that will strengthen consumer privacy protection.'
"CPOs are the public point people for a company's privacy initiatives. In other words, they function as the human face that is responsible for protecting the customer data that's collected and stored by companies.

"Some companies may be tempted to create a position with combined security and privacy duties because the areas are undoubtedly interlinked. However, the CPO position has a different posture than the CSO job. CPOs tend to be more outward facing, while CSOs look more inward."
"CPOs need to know technology, but they also need good public relations and policy skills. Federal regulations such as the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act (HIPAA) have forced companies to face privacy head-on. Gregory, however, sees identity theft as one of the prime influencers for the CPO position. People want to know how companies are protecting their sensitive information from the scourge, he said.
"The CPO position does have something in common with the CSO job: confusion over where they fit in the organizational structure. Do they answer to the CEO and the board of directors? Should they report to the CIO? The way a company answers such questions often says something about how much it truly values privacy (or security, for that matter).
"To be truly effective, a CPO shouldn't answer to the CIO, Gregory said. Such an arrangement would lessen the CPO's value because the CIO's main concern is business operations, not privacy. A model arrangement would entail the CPO, CIO and CSO all being on about the same level. 'They would have to use their negotiating skills to get the best thing for the business,' he said. 'In essence, you would have a quasi-balance of power under that arrangement.'"
+ More at:
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci874297,00.html

Patient Records: After the Bankruptcy

"Hundreds of thousands of Southern Californians are in danger of having their medical records destroyed because a company says it is no longer being paid to store them. Iron Mountain has been housing the records of KPC Medical Management, which closed its clinics in 2000 and left behind 8 million medical documents. After state regulators ordered the records made available for cancer patients and others currently receiving treatment, insurance companies put up about $2 million for distribution and storage. But the money ran out last summer.
"Iron Mountain has no immediate plans to destroy the documents, but urged former KPC patients to request their records. … the company, which charges $21.50 to send the documents, receives 300 to 400 such requests each month. The state Department of Managed Health Care has not had jurisdiction over the records since a bankruptcy court ordered the records transferred to Iron Mountain from another company…
"KPC, which was based in Anaheim, was the largest for-profit medical group in Southern California when it closed in 2000.
+ More at:
http://cbs.marketwatch.com/tools/quotes/newsArticle.asp?guid={6D064731

-E499-417E-A9F0-1E0A95E7B24A}&siteid=mktw&archive=thirdtrue
(registration required)

Consultants: Certification?

"HIPAA certifications are designed to do one thing: separate you from your money, according to Bernard (Bernie) Cowens, vice president of security services at Rainbow eSecurity. …He said that every time a new technology, regulation, or fad-du-jour comes along, a certification is sure to follow. He compared many certifications to multi-level marketing. 'Once an individual gets a particular certification, it is in his or her best interest to rabidly promote that certification,' he said. 'The more people who get a particular certification, the more legitimate it must be, right?'

Cowens isn't alone in his opinion of the certifications. While consultants have seen the Health Insurance Portability and Accountability Act (HIPAA) as a potential bright spot during the past few years, several experts we contacted cast doubt on the value of HIPAA-related certifications…
"Dennis Melamed agreed with Cowens, especially in the security arena. Melamed is the publisher of Health Information Privacy Alert, a trade publication focused on HIPAA and health data privacy and security issues. He said that from an IT security perspective, HIPAA certification seems unnecessary because HIPAA's security rules simply represent general good business practices, so IT pros should just focus on more general certification in security issues. 'Security is security is security, regardless of whether it is provoked by HIPAA regulations or the market,' Melamed said. He added that '…trying to dress up resumes with 'HIPAA-compliant' credentials may provoke more suspicion than trust.'"
+More at:
http://www.techrepublic.com/article.jhtml?id=r00720030212bla01.htm&fromtm=e101-2#
COMMENTARY: We agree with the comments about certification. If your objective is to be secure, we even agree with the notion that "security is security." However, HIPAA requires both security and compliance. You need consultants who know security and HIPAA or you need a team that can provide both.

Conferences and Webinars

On July 2, last year, almost 500 people joined us on a Webinar hosted by Search Security. [Issue 38] We have been invited to take another look at HIPAA and will be presenting **'Where Are We and Where Are We Going.' A look at HIPAA just before the deadline for the implementation of the first of the HIPAA regulations. The date is March 17**. Details in upcoming issues.

Sixth National HIPAA Summit Features Leading Healthcare Privacy & HIPAA Regulators -- March 26-28, 2003; Washington DC. For registration

Information call 800-684-4549 or email: registrationhq@aol.com. You may register with secure online registration and additional information at http://www.hipaasummit.com

_____